We claim:

1. A method of receiving real-time multimedia via a network, comprising the steps of:

transmitting a request for the multimedia from a client interface, wherein the request obtains a reply response containing a control message having a first encryption key, a unique software identifier containing an entitlement message, which has a second encryption key, the control message defining content stream information and access criteria, and the entitlement message defining the client interface entitlement rights; and

receiving the reply, wherein the unique software identifier decrypts the multimedia in real-time, in accordance with the content stream information and access criteria, in order to render the multimedia at the client interface.

2. The method according to claim 1, wherein the unique software identifier is a virtual smart card.

3. The method according to claim 1, wherein the first encryption key and the second encryption key are symmetric encryption pairs.

4. The method according to claim 1, wherein the first encryption key protects the multimedia and permits the multimedia to be descrambled.

5. The method according to claim 1, wherein the second encryption key protects the entitlement rights and permits the rendering of the multimedia at the client interface.

6. The method according to claim 1, wherein the multimedia includes audio or video.

7. A method of providing real-time multimedia via the Internet, comprising the steps of:

receiving a request for multimedia;

validating the request;

if said request is authorized in the validating step, generating a reply response containing a control message having a first encryption key, a unique software identifier containing an entitlement message which has a second encryption key, the control message defining content stream information and access criteria, and the entitlement message defining the user interface entitlement rights; and

transmitting the reply response, the reply response being configured so that the unique software identifier decrypts the multimedia in real-time, in accordance with the content stream information and access criteria, in order to render the multimedia at the client interface.

8. The method according to claim 7, wherein the unique software identifier is a virtual smart card.

9 The method according to claim 7, wherein the first key and the second key are symmetric encryption pairs.

10 The method according to claim 7, wherein the first key protects the multimedia and permits the multimedia to be descrambled.

11. The method according to claim 7, wherein the second key protects the entitlement rights and permits the rendering of the multimedia at the client interface.

12. The method according to claim 7, wherein the multimedia includes audio or video.

13. A system for providing real-time multimedia:

a media source configured to generate an audio/video content stream;

a code generator configured to generate a plurality of distinct codes, a unique software identifier, and a plurality of messages;

a media encoder configured to convert the audio/video content stream to a particular format and to provide non-encrypted multimedia to a media encryptor;

a media encryptor configured to dynamically encrypt the non-encrypted multimedia with at least one distinct code and to transmit the encrypted multimedia to a media server;

a media server configured to store the encrypted multimedia and to provide the encrypted multimedia stream link to a web server;

a web server configured to register an end-user and to provide an encrypted multimedia stream link to the end-user; and

an end-user configured to receive the encrypted multimedia stream link and, wherein the unique software identifier is configured to decrypt the encrypted multimedia in real-time in order to render the multimedia at the end-user.

14. The system according to claim 13, wherein the unique software identifier is a virtual smart card.

15. The system according to claim 13, wherein the messages include a control message and an entitlement message.

16. The system according to claim 15, wherein the control message defines content stream information and access criteria, and the entitlement message defines the end-user entitlement rights.

17. The system according to claim 13, wherein the plurality of distinct codes include a first key and a second key.

18. The system according to claim 17, wherein the first and second keys are symmetric encryption pairs.

19. The system according to claim 17, wherein the first key protects the multimedia and permits the multimedia to be descrambled at the end-user.

20. The system according to claim 17, wherein the second key protects entitlement rights and permits the rendering of the multimedia at the end-user.

21. The system according to claim 17, wherein the first key is embedded in the control message.

22. The system according to claim 17, wherein the second key is embedded in the entitlement message.

23. The system according to claim 14, wherein the virtual smart card is a software functional equivalent of a physical smart card.

24. A method of providing broadcast content security, comprising the steps of:

registering with a web content provider;

requesting broadcast content from the web content provider;

requesting a software voucher from a media operator;

at a key bank, receiving and validating the request, then generating the activation code and a unique software identifier; and

sending the activation code and the unique software identifier to the end-user and storing the activation code corresponding to the previous voucher.

25. The method of providing broadcast content security according to claim 24, wherein the unique software identifier is in the form of a virtual smart card with an entitlement management message.

26. The method according to claim 24, wherein the software voucher is digitally signed so that the rights management control center can verify whether the request originated from a valid web server.

27. The method according to claim 24, wherein the broadcast content includes audio and video signals.

28. A method of accessing encrypted broadcast content stream, comprising the steps of:

selecting an encrypted broadcast content stream;

checking the entitlement of the encrypted broadcast content stream;

determining whether an end-user has entitlement corresponding to the encrypted broadcast content stream by means of a unique software identifier and an activation code;

sending a link for the encrypted broadcast content stream to the end-user; and

decrypting the encrypted broadcast content stream.

29. The method according to claim 28, wherein the unique software identifier is in the form of a virtual smart card with an entitlement management message.

30. The method according to claim 28, wherein the broadcast content stream includes audio or video.

31. A system for dynamically receiving and displaying encrypted multi-media content, said system comprising:

a client interface coupled with a network, said client interface configured to generate a request for said content, wherein the request obtains a reply response containing a control message having a first encryption key, a unique software identifier containing an entitlement message, which has a encryption second key, the control message defining content stream information and access criteria, and the entitlement message defining the user interface entitlement rights, and

wherein the client interface is configured to download the reply response and decrypt the multimedia in real-time, in accordance with the content stream information and access criteria, in order to render the multimedia at the client interface.

32. The system according to claim 31, wherein the unique software identifier is a virtual smart card.

33. The system according to claim 31, wherein the first encryption key and the second encryption key are symmetric encryption pairs.

34. The system according to claim 31, wherein the first encryption key protects the multimedia and permits the multimedia to be descrambled.

35. The system according to claim 31, wherein the second encryption key protects the entitlement rights and permits the rendering of the multimedia at the client interface.

36. The system according to claim 31, wherein the multimedia includes audio or video.

37. The system according to claim 31, wherein the virtual smart card is a software functional equivalent of a physical smart card.

38. A system for dynamically providing and displaying encrypted multi-media content comprising:

a network server configured to receive and validate a request for multimedia;

an encryption component in communication with the network server and configured to generate a reply in response to the request, said response containing a control message having a first encryption key, a unique software identifier containing an entitlement message which has a second encryption key, the control message defining content stream information and access criteria, and the entitlement message defining the user interface entitlement rights; and

wherein the unique software identifier is configured to decrypt the multimedia in real-time, in accordance with the content stream information and acess criteria, in order to render the multimedia at a client interface.

39. The system according to claim 38, wherein the unique software identifier is a virtual smart card.

40. The system according to claim 38, wherein the first encryption key and the second encryption key are symmetric encryption pairs.

41. The system according to claim 38, wherein the first encryption key protects the multimedia and permits the multimedia to be descrambled.

42. The system according to claim 38, wherein the second encryption key protects the entitlement rights and permits the rendering of the multimedia at the client interface.

43. The system according to claim 38, wherein the multimedia includes audio and video.

44. A method for dynamically providing access control for broadcast content, comprising the steps of:

generating non-encrypted broadcast content;

configuring a plurality of distinct codes;

creating a unique software identifier;

generating a plurality of messages;

converting the broadcast content a particular format;

dynamically encrypting the broadcast content with at least one distinct code; and

transmitting the broadcast content to an end-user,

wherein the unique software identifier is configured to decrypt the broadcast content in real-time in order to render the broadcast content at the end-user.

45. The method according to claim 44, wherein the non-encrypted broadcast content is generated by a media source.

46. The method according to claim 44, wherein the plurality of distinct codes, the unique software identifier and the plurality of messages are generated by a code generator.

47. The method according to claim 44, wherein non-encrypted broadcast content is converted to a particular format by a media encoder.

48. The method according to claim 44, wherein the broadcast content is dynamically encrypted with at least one code by a media encryptor.

49. The method according to claim 44, wherein the unique software identifier is a virtual smart card.

50. The method according to claim 44, wherein the messages include a control message and an entitlement message.

51. The method according to claim 50, wherein the control message defines broadcast content stream information and access criteria, and the entitlement message defines the end-user entitlement rights.

52. The method according to claim 44, wherein the plurality of distinct codes include a first encryption key and a second encryption key.

53. The method according to claim 52, wherein the first and second encryption keys are symmetric encryption pairs.

54. The method according to claim 52, wherein the first encryption key protects the broadcast content and permits the broadcast content to be descrambled at the end-user.

55. The method according to claim 52, wherein the second encryption key protects entitlement rights and permits the rendering of the multimedia at the end-user.

56. The method according to claim 52, wherein the first encryption key is embedded in the control message.

57. The method according to claim 52, wherein the second encryption key is embedded in the entitlement message.

58. The method according to claim 44, wherein the broadcast content includes audio or video.

59. A system for providing real-time multimedia:

a means for generating an audio/video content stream;

a means for generating a plurality of distinct codes, a unique software identifier, and a plurality of messages;

a means for converting the audio/video content stream to a particular format and for providing non-encrypted multimedia to a media encryptor;

a means for dynamically encrypting the non-encrypted multimedia with at least one distinct code and to transmit the encrypted multimedia to a media server;

a means for storing the encrypted multimedia and to provide an encrypted multimedia stream link to a web server;

a means for registering an end-user and to provide the encrypted multimedia stream link to the end-user; and

a means for receiving the encrypted multimedia, wherein the unique software identifier is configured to decrypt the encrypted multimedia in real-time in order to render the multimedia at the end-user.

60. The system according to claim 59, wherein the unique software identifier is a virtual smart card.

61. The system according to claim 59, wherein the messages include a control message and an entitlement message.

62. The system according to claim 61, wherein the control message defines the content stream information, and the entitlement message defines the end-user entitlement rights.

63. The system according to claim 59, wherein the plurality of distinct codes include a first key and a second key.

64. The system according to claim 63, wherein the first and second keys are symmetric encryption pairs.

65. The system according to claim 63, wherein the first key protects the multimedia and permits the multimedia to be descrambled at the end-user.

66. The system according to claim 63, wherein the second key protects entitlement rights and permits the rendering of the multimedia at the end-user.

67. The system according to claim 63, wherein the first key is embedded in the control message.

68. The system according to claim 63, wherein the second key is embedded in the entitlement message.

69. The system according to claim 60, wherein virtual smart card is a software functional equivalent of a physical smart card.

70. A system for dynamically receiving and displaying encrypted multi-media content, said system comprising:

a means for interfacing coupled with a network, said interface means configured to generate a request for said content, wherein the request obtains a reply response containing a control message having a first encryption key, a unique software identifier containing an entitlement message, which has a encryption second key, the control message defining content stream information and access criteria, and the entitlement message defining the user interface entitlement rights,

wherein the interface means is configured to download the reply response and decrypt the multimedia in real-time, in accordance with the content stream information and access criteria, in order to render the multimedia at the interface means.

71. The system according to claim 70, wherein the unique software identifier is a virtual smart card.

72. The system according to claim 70, wherein the first encryption key and the second encryption key are symmetric encryption pairs.

73. The system according to claim 70, wherein the first encryption key protects the multimedia and permits the multimedia to be descrambled.

74. The system according to claim 70, wherein the second encryption key protects the entitlement rights and permits the rendering of the multimedia at the client interface.

75. The system according to claim 70, wherein the multimedia includes audio or video.

76. The system according to claim 70, wherein the virtual smart card is a software functional equivalent of a physical smart card.

77. A system for dynamically providing and displaying encrypted multi-media content comprising:

a means for receiving and validate a request for multimedia;

a means for encryption in communication with the receiving means and configured to generate a reply in response to the request, said response containing a control message having a first encryption key, a unique software identifier containing an

entitlement message which has a second encryption key, the control message defining content stream information and access criteria, and the entitlement message defining the user interface entitlement rights;

wherein the unique software identifier is configured to decrypt the multimedia in real-time, in accordance with the content stream information and access criteria, in order to render the multimedia at a client interface.

78. The system according to claim 77, wherein the unique software identifier is a virtual smart card.

79. The system according to claim 77, wherein the first encryption key and the second encryption key are symmetric encryption pairs.

80. The system according to claim 77, wherein the first encryption key protects the multimedia and permits the multimedia to be descrambled.

81. The system according to claim 77, wherein the second encryption key protects the entitlement rights and permits the rendering of the multimedia at the client interface.

82. The system according to claim 77, wherein the multimedia includes audio and video.